Security Analysis of mixFeed

Bishwajit Chakraborty and Mridul Nandi
Indian Statistical Institute, Kolkata

6th Nov 2019
Simplified AE (with no AD) based on a TBC $\tilde{E}_K$. 

\[
\begin{align*}
0^n & \rightarrow \tilde{E}_K \\
\text{(N,0,0)} & \rightarrow M_1 \\
\text{FB}^+ & \rightarrow \tilde{E}_K \\
\text{(N,1,0)} & \rightarrow M_2 \\
\text{FB}^+ & \rightarrow \tilde{E}_K \\
\text{(N, 2, } \delta \text{)} & \rightarrow T
\end{align*}
\]
Decryption: $FB^- (\text{instead of } FB^+)$.

Assume $C_i = M_i \oplus Y_i - 1$ and $X_i$ is dependent on $Y_i - 1$ and a significant fraction of bits of $C_i$.

Statistical Institute, Kolkata

TBC-based AE Mode

- Simplified AE (with no AD) based on a TBC $\tilde{E}_K$.

\[ 0^n \rightarrow \tilde{E}_K \rightarrow FB^+ \rightarrow \tilde{E}_K \rightarrow FB^+ \rightarrow \tilde{E}_K \rightarrow T \]

\[ (N,0,0) \rightarrow M_1 \rightarrow (N,1,0) \rightarrow M_2 \rightarrow (N,2,\delta) \]

- State size: (i) TBC state $n$, (ii) Tweak and Key state $t + k$, (iii) Possibly additional state to hold $t$-bit tweak and $k$ bit key.
TBC-based AE Mode

- Simplified AE (with no AD) based on a TBC $\tilde{E}_K$.

$$I$$

Assume $C_i = M_i \oplus Y_{i-1}$ and $X_i$ is dependent on $Y_{i-1}$ and a significant fraction of bits of $C_i$.

- State size: (i) TBC state $n$, (ii) Tweak and Key state $t + k$, (iii) Possibly additional state to hold $t$-bit tweak and $k$ bit key.

- Decryption: $FB^{-}$ (instead of $FB^{+}$).
TBC-based AE Mode

- Simplified AE (with no AD) based on a TBC $\tilde{E}_K$.

\[
\begin{align*}
0^n & \rightarrow \tilde{E}_K & (N,0,0) & \rightarrow M_1 & \rightarrow FB^+ & \rightarrow \tilde{E}_K & (N,1,0) & \rightarrow M_2 & \rightarrow FB^+ & \rightarrow \tilde{E}_K & (N,2,\delta) & \rightarrow T
\end{align*}
\]

- State size: (i) TBC state $n$, (ii) Tweak and Key state $t + k$, (iii) Possibly additional state to hold $t$-bit tweak and $k$ bit key.

- Decryption: $FB^-$ (instead of $FB^+$).

- Assume $C_i = M_i \oplus Y_{i-1}$ and $X_i$ is dependent on $Y_{i-1}$ and significant fraction of bits of $C_i$. 
I How small can 

\( \text{Adv}_{\text{TPRP}} (D, T) \) be? Cannot be better than 

\( \frac{T}{2} \).

I Can have weaker security while designing TBC from BC.

Statistical Institute, Kolkata

TBC-based AE Mode

\[
\begin{align*}
0^n \rightarrow &\quad \tilde{E}_K \rightarrow \tilde{E}_K \rightarrow \tilde{E}_K \rightarrow T \\
\text{(N,0,0)} \rightarrow &\quad M_1 \rightarrow \text{FB}^+ \rightarrow \text{FB}^+ \rightarrow \text{FB}^+ \\
\text{(N,1,0)} \rightarrow &\quad M_2 \rightarrow \text{FB}^+ \rightarrow \text{FB}^+ \rightarrow \text{FB}^+ \\
\text{(N,2,δ)} \rightarrow &
\end{align*}
\]

\[
\text{Adv}_{\text{AE}}^{\text{priv}} (D, T) \leq \text{Adv}_{\text{TPRP}}^{\text{priv}} (D, T) \quad \text{and} \quad \text{Adv}_{\text{AE}}^{\text{auth}} (D, T) \leq \text{Adv}_{\text{TPRP}}^{\text{auth}} (D, T) + O \left( \frac{D}{2^n} \right)
\]
TBC-based AE Mode

\[ \tilde{E}_K \quad (N,0,0) \quad \tilde{E}_K \quad (N,1,0) \quad \tilde{E}_K \quad (N,2,\delta) \]

\[ 0^n \quad \tilde{E}_K \quad \text{FB}^+ \quad \tilde{E}_K \quad \text{FB}^+ \quad \tilde{E}_K \quad T \]

\[ C_1 \quad M_1 \quad \text{FB}^+ \quad C_2 \quad M_2 \]

\[ \begin{align*}
\text{Adv}_{AE}^{priv}(D,T) & \leq \text{Adv}_{E}^{TPRP}(D,T) \\
\text{Adv}_{AE}^{auth}(D,T) & \leq \text{Adv}_{E}^{TPRP}(D,T) + \mathcal{O}(\frac{D}{2^n})
\end{align*} \]

- How small can \( \text{Adv}_{E}^{TPRP}(D,T) \) be? Cannot be better than \( T/2^k \).
- Can have weaker security while designing TBC from BC.
TBC based on BC
Some Examples of TBC based on BC

\[ K \]
\[ E \rightarrow G \rightarrow L \]
\[ N \]
\[ 2^i L \oplus \delta \]
\[ X \rightarrow E \rightarrow Y \]

Figure: ICE1 with KDF1. (Remus-N1). Here tweak = \((N, i, \delta)\).
Some Examples of TBC based on BC

- $D$ many queries to ICE1 with input $0^n$ and changing the tweak to get $Y_1, \ldots, Y_D$.
- $K_1, \ldots, K_D$: intermediate keys for the second call of BC.
Some Examples of TBC based on BC

- $D$ many queries to ICE1 with input $0^n$ and changing the tweak to get $Y_1, \ldots, Y_D$.
- $K_1, \ldots, K_D$: intermediate keys for the second call of BC.
- Precompute $T$ many blockcipher outputs $Y'_1, \ldots, Y'_T$ with input $0^n$ and key $K'_1, \ldots, K'_T$. 
Some Examples of TBC based on BC

- $D$ many queries to ICE1 with input $0^n$ and changing the tweak to get $Y_1, \ldots, Y_D$.

- $K_1, \ldots, K_D$: intermediate keys for the second call of BC.

- Precompute $T$ many blockcipher outputs $Y'_1, \ldots, Y'_T$ with input $0^n$ and key $K'_1, \ldots, K'_T$.

- When $DT \approx 2^n$, we expect $K_i = K'_j$ (detectable through $Y_i = Y'_j$).
Some Examples of TBC based on BC

Figure: ICE2 with KDF2. (Remus-N2). Here tweak = \((N, i, \delta)\).

- TPRP advantage of ICE2 is \(\frac{DT}{2^{2n}}\). Requires larger state.
- Can we have both (1) smaller state (2) higher security?
New Reduction and New Security Game

![Diagram](image)

**Figure:** ICE1 with $G$ as identity. (Remus-N1). Here tweak $= (N, i, \delta)$.

1. Use different reduction games considering $\mu$-respecting adversary (the maximum number of query to TBC with same input is at most $\mu$).

2. TPRP advantage of such an adversary against ICE1 is $\frac{\mu T}{2^n}$.

3. Restrict $\mu = O(n)$ and consider $n$-multicollision.
mixFeed
The mF Mode of AEAD

Figure: Block diagram of mF. $Fmt_1(A) = (A_2 || A_1)$, $Fmt_2(M) = (M_2 || M_1)$. 
FeedBack Function used in mF

\[ M = M^1 \parallel M^0 \]

\[ Y \xrightarrow{FB^+} X \]

\[ C = C^1 \parallel C^0 \]
The TBC in mixFeed

Figure: The tweakable block cipher in mixFeed. Here $\rho$ is the 11-th round key function in AES key scheduling algorithm.

1. State size is just $n + k$ (i.e. 256).
2. Rate is 1.
Domain Separation by Last block processing.

\[ \frac{M_m}{2} \rightarrow E \]

\[ \frac{C_m}{2} \rightarrow K_l \]

\[ \delta_M \rightarrow X_{l+1} \]

\[ T \rightarrow \]

\[ E \rightarrow K_{l+1} \]

**Figure:** MixFeed Last block processing.
Security Definitions of Input Restricting TPRP

- **Tweak space** $\mathcal{T}$. $n$-bit TBC $\tilde{E}$. Tweakable random Permutation $\tilde{\Pi}$.

- **$\mu$-TPRP:**
  - $\mathcal{A}^O$, Restriction: $\forall X \in \{0,1\}^n$ number of queries $(\cdot, X) \leq \mu$
  - $\text{Adv}_{\tilde{E}}^{\mu-\text{TPRP}}(\mathcal{A}) = \left| \Pr[\mathcal{A}\tilde{E}_k = 1] - \Pr[\mathcal{A}\tilde{\Pi} = 1] \right|$
  - $\text{Adv}_{\tilde{E}}^{\mu-\text{TPRP}}(q, t) = \max_{\mathcal{A}} \text{Adv}_{\tilde{E}}^{\mu-\text{TPRP}}(\mathcal{A})$

  where max over all $\mathcal{A}$ (number of queries $\leq q$, time $\leq t$).
A $\tilde{E}_K$ runs in two phase. In the first phase it is $\mu$-respecting.
(\(\mu, D\))-Multi-commitment-Prediction (or (\(\mu, D\))-mcp)

1. \(\mathcal{A}\tilde{\mathcal{E}}_K\) runs in two phase. In the first phase it is \(\mu\)-respecting.

2. \(\mathcal{A}\) commits \(D\) many \((tw_i, x_i, y_i)\), \(x_i, y_i \in \{0, 1\}\).
(μ, D)-Multi-commitment-Prediction (or (μ, D)-mcp)

1. \( \mathcal{A} \tilde{E}_K \) runs in two phase. In the first phase it is \( \mu \)-respecting.

2. \( \mathcal{A} \) commits \( D \) many \((tw_i, x_i, y_i)\), \( x_i, y_i \in \{0, 1\}^2 \).

3. **Phase II:** \( \mathcal{A} \tilde{E}_K \) (with no restriction making at most \( D \) queries including prediction) predicts fresh some \((tw_j, X_j, y_j)\) where \( \left\lfloor X_j \right\rfloor \frac{n}{2} = x_i \).
\((\mu, D)\)-Multi-commitment-Prediction (or \((\mu, D)\)-mcp)

1. \(\mathcal{A} \tilde{E}_K\) runs in two phase. In the first phase it is \(\mu\)-respecting.

2. \(\mathcal{A}\) commits \(D\) many \((tw_i, x_i, y_i), x_i, y_i \in \{0, 1\}^n\).

\[tw_i\]

\(?\)

\[x_i\]

\[y_i\]

\[\tilde{E}_K\]

Phase II: \(\mathcal{A} \tilde{E}_K\) (with no restriction making at most \(D\) queries including prediction) predicts \textbf{fresh} some \((tw_j, X_j, y_j)\) where \(\left\lceil X_j \right\rceil \frac{n}{2} = x_i\).

3. \(\mathcal{A}\) wins \((\mu, D)\)-mcp game if \(\left\lceil \tilde{E}_K(tw_j, X_j) \right\rceil \frac{n}{2} = y_j\), i.e. correctly predicts,
mcp Security Game

\[ \text{Adv}^{(\mu,D)-\text{mcp}}_{\tilde{E}} (\mathcal{A}) = \Pr [\mathcal{A} \text{ wins } (\mu,D)-\text{mcp} \text{ game }] \]

\[ \text{Adv}^{(\mu,D)-\text{mcp}}_{\tilde{E}} (T) = \max_{\mathcal{A}} \text{Adv}^{(\mu,D)-\text{mcp}}_{\tilde{E}} (\mathcal{A}) \]

Where max over all \( \mathcal{A} \) with runtime at most \( T \) (this includes the number of public primitive queries).
μ-Multicollision Game

- \( A^{\mathcal{O}E_k} \)

- \( A \) wins \( \mu \)-multicollision game if
  - \( A \) makes \( \mu \) many queries \((X_i, Y_i)_{i \in [1, \mu]}\) with \( Y_i = Y_j \ \forall i, j \in [1, \mu] \) among all \( D \) queries.

- \( \text{Adv}^{\mu \text{-mult}}(A) = \Pr[ A \text{ wins } \mu \text{-multicollision game}] \)

\[
\text{Adv}^{\mu \text{-mult}}(D) = \max_{A} \text{Adv}^{\mu \text{-mult}}(A)
\]

Where \( \max \) over all \( A \) (number of queries \( \leq D \)).
\(\mu\)-Multicollision Game

Let \(P\) be the ideal \(n\) bit random permutation and \(P'\) is the \(n/2\)-bit truncated function of \(P\).

**Theorem**

\[
\text{Adv}_{P'}^{\mu\text{-mcoll}}(D) \leq D \left(1 + \frac{\mu^2}{2^n}\right) \left(\frac{D}{2^{n/2}}\right)^{\mu-1}.
\]

When \(\mu = n\),

\[
\text{Adv}_{P'}^{n\text{-mcoll}}(D) = O\left(\frac{D}{2^{n/2}}\right).
\]
Security Reductions of mixFeed
\( \mathcal{B} \): privacy adversary of \( mF \).

\( \mathcal{A} \): \( \mu \)-TPRP adversary of \( \tilde{E} \).

\( \mathcal{C} \): multicollision adversary.

**Theorem**

\[
\text{Adv}_{mF}^{\text{priv}}(\mathcal{B}) \leq \text{Adv}_{\tilde{E}}^{\mu-\text{TPRP}}(\mathcal{A}) + \text{Adv}_{P}^{\mu+1-\text{mcoll}}(\mathcal{C}).
\]

So,

\[
\text{Adv}_{mF}^{\text{priv}}(D, T) \leq \text{Adv}_{\tilde{E}}^{n-\text{TPRP}}(D, T) + O(D/2^n)^2).
\]
For any \((D, T)\) forging adversary \(B\) of \(mF\) we have.

(i) \((\mu - 1, D)\)-mcp adversary \(A\) and (ii) \(C\) with oracle \(O_{\tilde{E}_K}\) where 

\[ O_{\tilde{E}}(tw, X, C) \rightarrow X' := C \oplus (0^n \| \tilde{E}_K(tw, X) \| n). \]

**Theorem**

For any forging adversary \(B\) of \(mF\) with data complexity \(D\) there is (i) an \((\mu - 1, D)\)-mcp adversary \(A\) of \(\tilde{E}\), and (ii) an \(\mu + 1\)-multicollision adversary \(C\) as defined above, we have

\[
\text{Adv}_{mF}^{\text{forge}}(B) \leq \text{Adv}_{\tilde{E}}^{(\mu - 1, D)\text{-mcp}}(A) + \text{Adv}_{O_{\tilde{E}_K}}^{(\mu + 1)\text{-mcoll}}(C).
\]
The TBC in mixFeed

(i) $\mu$-respecting TPRP  
(ii) $(\mu, D)$-mcp advantage and  
(iii) $(\mu + 1)$-multi-collision.

Assumption

For any $K \in \{0, 1\}^n$ chosen uniformly at random, probability that $K$ has a period at most $l$ is at most $\frac{l}{2^n}$.  

For random permutation the probability is much smaller: $\frac{l}{2^n}$.  

Bishwajit Chakraborty and Mridul Nandi  
Indian Security Analysis of mixFeed  
6th Nov 2019
Theorem

Under the above assumption

\[
\text{Adv}^{(\mu,D)-\text{mcp}}_E(T) = O\left(\frac{D}{2^{n^2}}\right) + O\left(\frac{nT}{2^n}\right)
\]

\[
\text{Adv}^{n-\text{TPRP}}_E(D, T) = O\left(\frac{D}{2^{n^2}}\right) + O\left(\frac{nT}{2^n}\right).
\]

\[
\text{Adv}^{n-\text{mcoll}}_E(D) \leq O\left(\frac{D}{2^{n^2}}\right).
\]
Theorem (Final Bound of mixFeed)

Under Assumption 1

\[ \text{Adv}_{\text{mixFeed}}^{\text{priv}}(D, T) = O\left(\frac{D}{2^n}\right) + O\left(\frac{nT}{2^n}\right) \]

\[ \text{Adv}_{\text{mixFeed}}^{\text{forge}}(D, T) = O\left(\frac{D}{2^n}\right) + O\left(\frac{nT}{2^n}\right) \]
Conclusion: mixFeed Mode of AEAD

- mixFeed is provable secure under the NIST requirements (by Assumption 1) in the nonce respecting scenario.

- As shown by Mustafa Khairallah (in the Forum), mixFeed is vulnerable to Nonce misuse attacks.

- the re-keying is done simply by the AES key scheduling algorithm and can be done online. So minimal state size.

- The Feedback function is extremely simple as it requires only $n$-bit XOR.
Conclusion: mixFeed Mode of AEAD

- mixFeed is provable secure under the NIST requirements (by Assumption 1) in the nonce respecting scenario.
- As shown by Mustafa Khairallah (in the Forum), mixFeed is vulnerable to Nonce misuse attacks.
- the re-keying is done simply by the AES key scheduling algorithm and can be done online. So minimal state size.
- The Feedback function is extremely simple as it requires only $n$-bit XOR.

Thank You!